
**Vendor:** Cisco

**Exam Code:** 300-206

**Exam Name:** Implementing Cisco Edge Network Security Solutions

**Version:** DEMO

**QUESTION 1**
How much storage is allotted to maintain system,configuration , and image files on the Cisco ASA 1000V during OVF template file deployment?

A. 1GB
B. 5GB
C. 2GB
D. 10GB

**Answer:** C

**QUESTION 2**
Which two option are protocol and tools are used by management plane when using cisco ASA general management plane hardening ?

A. Syslog
B. Netflow
C. Icmp unreachabl
D. Cisco url filtering

**Answer:** AB
**Explanation:**
http://www.cisco.com/web/about/security/intelligence/firewall-best-practices.html

General Management Plane Hardening
The purpose of the management plane is to provide the capability to access, configure, and manage a device and to monitor its operations and the network on which it is deployed. The management plane receives and sends traffic for these functions. One must secure both the management plane and control plane of a device because operations of the control plane directly affect operations of the management plane. The following is a list of common protocols and tools used by the management plane:

- SNMP
- Telnet
- SSH
- FTP
- TFTP
- SCP
- TACACS+
- RADIUS
- NetFlow
- Network Time Protocol (NTP)
- Syslog

**QUESTION 3**
When a Cisco ASA CX module is management by Cisco Prime Security Manager in a Multiple Devices Mode, which mode does the firewall use ?

A. Managed Mode
B. Unmanaged mode
C. Single mode
D. Multi mode

**Answer:** A
**Explanation:**
http://www.cisco.com/c/en/us/td/docs/security/asacx/9-1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1b_User_Guide_for_ASA_CX_and_PRSM_9_1_chapter_011 0.html#task_7E648F43AD724DA2983699B12E92A528

### Managing CX Devices in Multiple Device Mode

If you manage a CX device in PRSM Multiple Device mode, the device is placed in **managed mode**.

When a CX device is in managed mode, you cannot configure it directly through its web interface in Single Device mode. All configuration and monitoring must be done through PRSM Multiple Device mode. The only exception is that the local CLI is still available, where you can troubleshoot and fix basic configuration settings such as IP addressing, DNS, NTP, and passwords.

**Putting a CX Device into Managed Mode**

To put an ASA CX into managed mode, you add the ASA that contains the ASA CX SSP to the device inventory.

Upon successful device configuration discovery, the CX device is placed in managed mode.

Tip If the CX believes that it is already being managed by a different PRSM server, discovery will fail, because you cannot manage a single CX device from multiple PRSM servers. If this happens, log into the CX web interface in Single Device mode and click the link to unmanage the device. Then try again to add the device to the inventory (delete it first if necessary).

**QUESTION 4**
Which statement about the configuration of the Cisco ASA NetFlow v9 (NSEL) is true ?

A. To view bandwidth usage for the NetFlow record, you must enable QoS features
B. Use sysopt command to enable NSEL on a specific interface
C. NSEL can be used without a collector configured
D. NSEL tracks the flow continuously and provides updates every 10 seconds
E. You must define a flow-export event type under a policy

**Answer:** E
**Explanation:**
http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/monitor_nsel.html

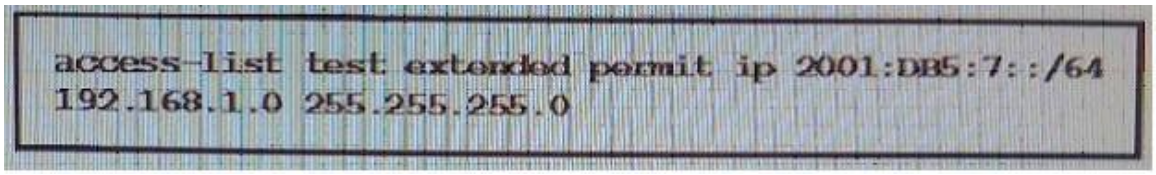
- If you have previously configured flow-export actions using the **flow-export enable** command, and you upgrade to a later version, then your configuration is automatically converted to the new Modular Policy Framework **flow-export event-type** command, which is described under the **policy-map** command.
- Flow-export actions are not supported in interface-based policies. You can configure flow-export actions in a class-map only with the **match access-list**, **match any**, or **class-default** commands. You can only apply flow-export actions in a global service policy.
- To view bandwidth usage for NetFlow records (not available in real-time), you must use the threat detection feature.

**QUESTION 5**
What is a required attribute to configure NTP authentication on a Cisco ASA?

A. Key ID
B. IPsec
C. AAA
D. IKEv2

**Answer:** A

**QUESTION 6**
Refer to the exhibit. Which statement about this access list is true?



A. This access list does not work without 6to4 NAT
B. IPv6 to IPv4 traffic permitted on the Cisco ASA by default
C. This access list is valid and works without additional configuration
D. This access list is not valid and does not work at all
E. We can pass only IPv6 to IPv6 and IPv4 to IPv4 traffic

**Answer:** D

**QUESTION 7**
Which statement about Dynamic ARP Inspection is true ?

A. In a typical network, you make all ports as trusted expect for the ports connection to switches , which are untrusted
B. DAI associates a trust state with each switch
C. DAI determines the validity of an ARP packet based on valid IP to MAC address binding from the DHCP snooping database
D. DAI intercepts all ARP requests and responses on trusted ports only
E. DAI cannot drop invalid ARP packets

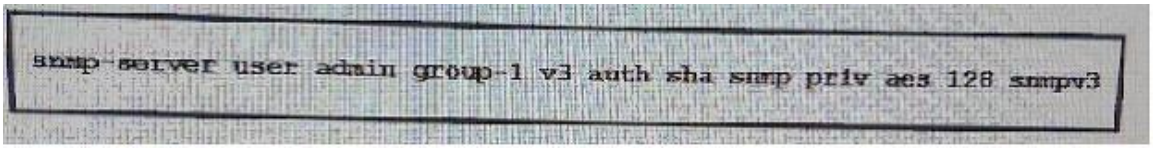
**Answer:** C

**QUESTION 8**
What can an administrator do to simultaneously capture and trace packets in a Cisco ASA?

A. Install a Cisco ASA virtual appliance.
B. Use the trace option of the capture command.
C. Use the trace option of the packet-tracer command.
D. Install a switch with a code that supports capturing, and configure a trunk to the Cisco ASA.

**Answer:** B

**QUESTION 9**
Refer to the exhibit. This command is used to configure the SNMP server on a Cisco router.
Which option is the encryption password for the SNMP server?




A. Sha
B. Snmp
C. Group-1
D. Snmpv3

**Answer:** B

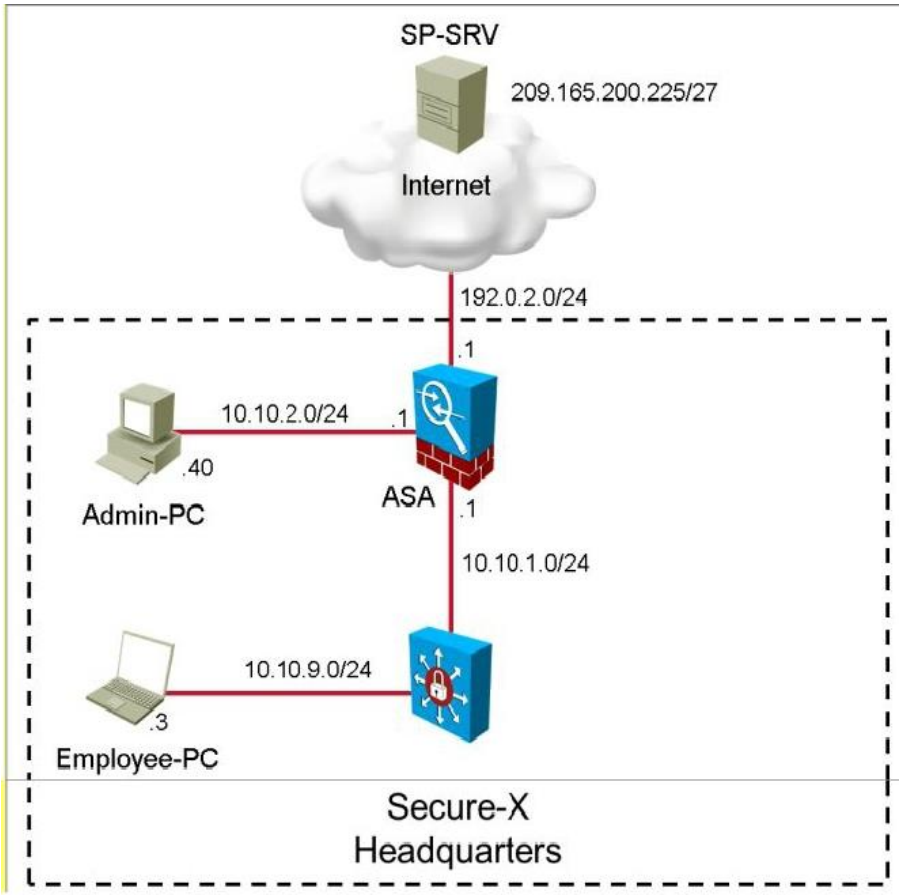
**QUESTION 10**
You are the network security engineer for the Secure-X network. The company has recently detected Increase of traffic to malware Infected destinations. The Chief Security Officer deduced that some PCs in the internal networks are infected with malware and communicate with malware infected destinations.
The CSO has tasked you with enable Botnet traffic filter on the Cisco ASA to detect and deny further connection attempts from infected PCs to malware destinations. You are also required to test your configurations by initiating connections through the Cisco ASA and then display and observe the Real-Time Log Viewer in ASDM.
To successfully complete this activity, you must perform the following tasks:

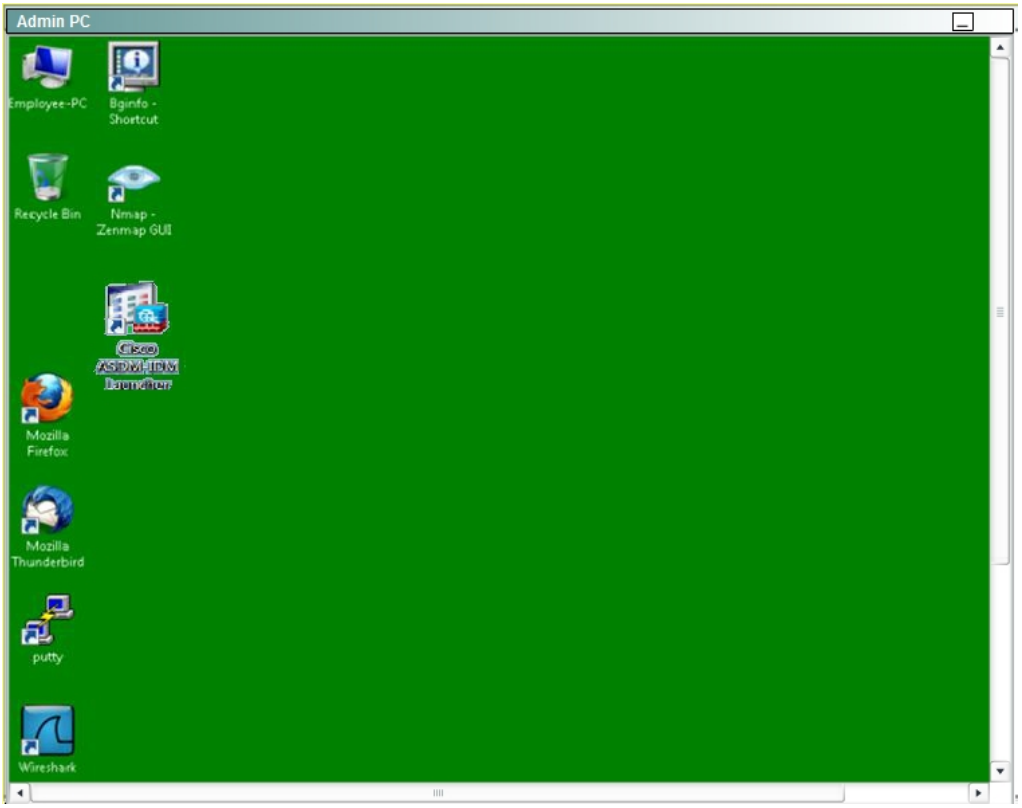
```
- Download the dynamic database and enable use of it.
- Enable the ASA to download of the dynamic database
- Enable the ASA to download of the dynamic database.
- Enable DNS snooping for existing DNS inspection service policy
rules..
- Enable Botnet Traffic Filter classification on the outside interface
for All Traffic.
- Configure the Botnet Traffic Filter to drop blacklisted traffic on
the outside interface. Use the default Threat Level settings
```

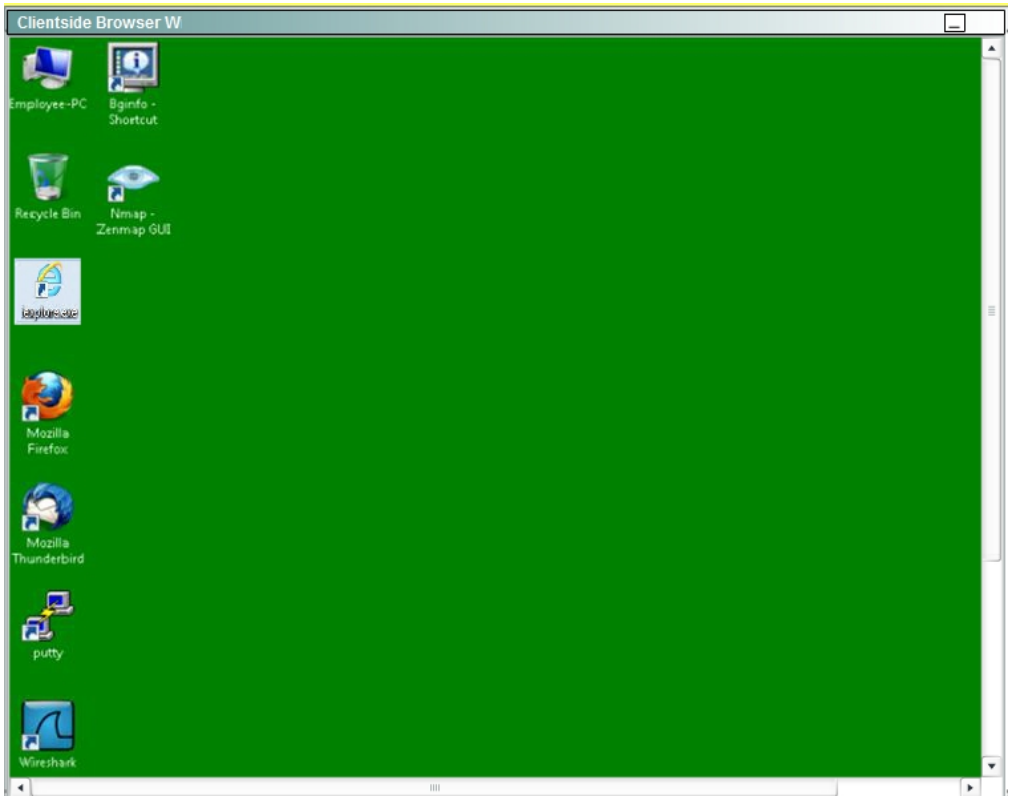
NOTE: The database files are stored in running memory; they are not stored in flash memory.
NOTE: DNS is enabled on the inside interface and set to the HQ-SRV (10.10.3.20).
NOTE: Not all ASDM screens are active for this exercise.

```
- Verify that the ASA indeed drops traffic to blacklisted destinations
by doing the following:
- From the Employee PC, navigate to http://www.google.com to make sure
that access to the Internet is working.
- From the Employee PC, navigate to http://bot-sparta.no-ip.org. This
destination is classified as malware destination by the Cisco SIO
database.
- From the Employee PC, navigate to http://superzarabotok-gid.ru/. This
destination is classified as malware destination by the Cisco SIO
database.
- From Admin PC, launch ASDM to display and observe the Real-Time Log
Viewer.
```

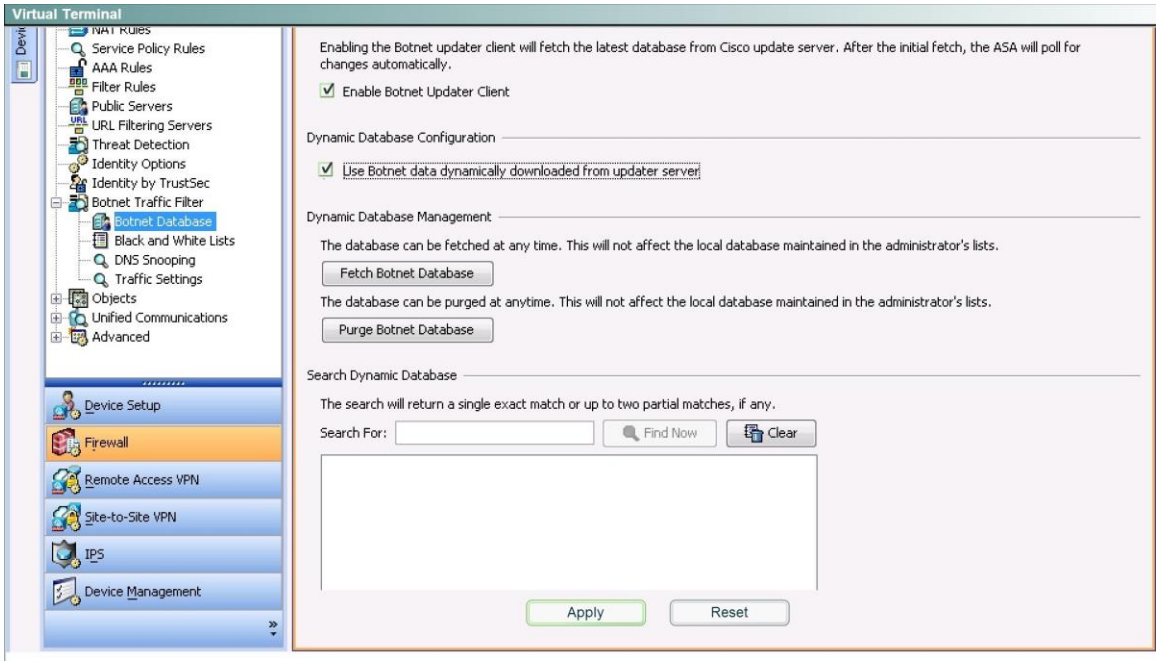
You have completed this exercise when you have configured and successfully tested Botnet traffic filter on the Cisco ASA.


SP-SRV
209.165.200.225/27
Internet
192.0.2.0/24
.1
10.10.2.0/24
.1
.40
Admin-PC
ASA
.1
10.10.1.0/24
10.10.9.0/24
.3
Employee-PC
Secure-X
Headquarters


Admin PC
Employee-PC
Bginfo - Shortcut
Recycle Bin
Nmap - Zenmap GUI
Cisco ASDM-IDM Launcher
Mozilla Firefox
Mozilla Thunderbird
putty
Wireshark




See the explanation for detailed answer to this sim question.
First, click on both boxes on the Botnet Database as shown below and hit apply:




**QUESTION 11**

If you disable PortFast on switch ports that are connected to a Cisco ASA and globally turn on BPDU filtering, what is the effect on the switch ports?

A. The switch ports are prevented from going into an err-disable state if a BPDU is received.
B. The switch ports are prevented from going into an err-disable state if a BPDU is sent.
C. The switch ports are prevented from going into an err-disable state if a BPDU is received and sent.
D. The switch ports are prevented from forming a trunk.

**Answer:** C

**QUESTION 12**
Which cloud characteristic is used to describes the sharing of physical resource between various entities ?

A. Elasticity
B. Ubiquitous access
C. Multitenancy
D. Resiliency

**Answer:** D
**Explanation:**
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_12-3/123_cloud1.html

**QUESTION 13**
Which option lists cloud deployment models?

A. Private, public, hybrid, shared
B. Private, public, hybrid
C. IaaS, PaaS, SaaS
D. Private, public, hybrid, community

**Answer:** D
**Explanation:**
https://www.ibm.com/developerworks/community/blogs/722f6200-f4ca-4eb3- 9d64-8d2b58b2d4e8/entry/4_Types_of_Cloud_Computing_Deployment_Model_You_Need_to_K now1?lang=en

# Thank You for Trying Our Product

## Lead2pass Certification Exam Features:


★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.


★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

**10% Discount Coupon Code:** **ASTR14**